NASKAH PUBLIKASI

ANALISIS PERFORMENCE JARINGAN NIRKABEL MENGGUNAKAN *AIRCRACK-NG* DAN *WIRESHARK*

Diajukan untuk Memenuhi Tujuan dan Syarat-Syarat Guna Memperoleh Gelar Sarjana Teknik pada Fakultas Teknik Jurusan Teknik Elektro Universitas Muhammadiyah Surakarta

OLEH :

NAMA : WASIS UNGGUL SAPUTRO
NIM : D 400 070 015
NIRM :

JURUSAN ELEKTRO FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2013

HALAMAN PENGESAHAN

Tugas Akhir dengan judul "**ANALISIS PERFORMANCE JARINGAN NIRKABEL MENGGUNAKAN *AIRCRACK-NG* DAN *WIRESHARK***" ini telah dipertahankan dan dipertanggung jawabkan di hadapan Dewan Penguji Tugas Akhir Fakultas Teknik Jurusan Teknik Elektro Universitas Muhammadiyah Surakarta, pada :

Hari :

Tanggal :

Dewan Penguji:

1. M. Kusban, S.T, M.T. .....
2. Umi Fadlilah, S.T, M.Eng. .....
3. Agus Supardi, S.T, M.T. .....
4. Ratnasari, S.T, M.T .....

Mengetahui,

Dekan Fakultas Teknik Universitas Muhammadiyah Surakarta	Ketua Jurusan Teknik Elektro Universitas Muhammadiyah Surakarta
(Ir. Agus Riyanto, M.T.)	(Ir. Jatmiko, M.T.)

ANALISIS PERFORMENCE JARINGAN NIRKABEL MENGGUNAKAN *AIRCRACK-NG* DAN *WIRESHARK*

Wasis Unggul Saputro
Fakultas Teknik Jurusan Teknik Elektro Universitas Muhamadiyah Surakarta
Jl. A. Yani Tromol Pos 1 Pabelan, Kartasura - Surakarta

ABSTRAKSI

Industri WLAN 802.11 atau WiFi (Wireless Fidelity) pada saat ini sedang berkembang dan sedang mendapatkan momentumnya. Berbagai macam toko, rumah sakit, bandara, mall, cafe, kantor dan tempat pendidikan sudah banyak memanfaatkan teknologi WiFi untuk berkomunikasi. Teknologi ini digunakan karena mobilitas dan produktivitas tinggi sehingga memudahkan penggunanya dalam berkomunikasi tanpa koneksi fisik. WLAN memungkinkan client untuk mengakses informasi secara realtime sepanjang masih dalam jangkauan WLAN, sehingga meningkatkan kualitas layanan dan produktivitas. Pengguna bisa melakukan kerja dimanapun berada asal dilokasi tersebut masuk dalam coverage area WLAN.

Kekuatan sinyal juga sangat berpengaruh dalam hal pertukaran data, karena jika terjadi hal sinyal pada jaringan hots port full tapi kekuatan download dan upload lemah maka dapat disimpulkan beberapa penyebabnya diantaranya adalah : banyak yang mengunakan jaringan tersebut, alat rusak, atau juga jaringan digunakan oleh pihak itu.

Aircrack-ng dan wireshark adalah salah satu software yang berbasis open source. Software ini terbilang baru dan masih jarang digunakan oleh banyak orang.

Kata kunci : *performance jaringan nirkabel, aircrack-ng, dan wireshark*

1. PENDAHULUAN

Industri WLAN 802.11 atau *WiFi* (*Wireless Fidelity*) pada saat ini sedang berkembang dan sedang mendapatkan momentumnya. Berbagai macam toko, rumah sakit, bandara, mall, cafe, kantor dan tempat pendidikan sudah banyak memanfaatkan teknologi *WiFi* untuk berkomunikasi. Teknologi ini digunakan karena mobilitas dan produktivitas tinggi sehingga memudahkan penggunanya dalam berkomunikasi tanpa koneksi fisik. WLAN memungkinkan *client* untuk mengakses informasi secara *realtime* sepanjang masih dalam jangkauan WLAN, sehingga meningkatkan kualitas layanan dan *produktivitas*. Pengguna bisa melakukan kerja dimanapun berada asal dilokasi tersebut masuk dalam *coverage area* WLAN.

Sistem keamanan pada suatu jaringan menjadi salah satu hal penting dalam sistem informasi. Keamanan jaringan biasanya tidak terlalu diperhatikan oleh pemilik sistim informasi ataupun pengelolanya. Keamanan jaringan biasanya menjadi

prioritas terakhir untuk diperhatikan, bahkan sekalipun terjadi penurunan kemampuan kerja komputer. Jika hal tersebut terjadi maka pemilik pada umumnya akan mengurangi aspek keamanan atau bahkan aspek keamanan akan ditiadakan untuk tujuan mengurangi beban kerja komputer. Konsekuensinya peniadaan sistem keamanan memungkinkan informasi penting dan rahasia dapat diketahui oleh pihak lain. Hal buruk lain yang dapat terjadi misalnya informasi penting tersebut dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengeruk keuntungan sendiri bahkan dapat merusak kinerja pemilik informasi. Kejahatan seperti itu biasanya dilakukan langsung terhadap sistem keamanan yang bersifat fisik, sistim keamanan yang berhubungan dengan personal, keamanan data dan media serta teknik komunikasi dan keamanan operasi.

Melihat berbagai ancaman dan isu-isu kemanan yang terdapat pada jaringan *wireless*, maka diperlukan sistem kemanan yang memadai. Pada intinya, aspek keamanan jaringan *wireless* mempunyai beberapa lingkup yang penting, yaitu:

a. Privacy & Confidentiality

Hal yang paling penting dalam aspek ini adalah usaha untuk menjaga data dan informasi dari pihak yang tidak diperbolehkan mengkasesnya. *Privacy* lebih mengarah kepada data-data yang sifatnya privat. Sebagai contoh, email pengguna yang tidak boleh dibaca admin.

b. Integrity

Aspek ini mengutamakan data atau informasi tidak boleh di akses tanpa seizin pemiliknya. Sebagai contoh, sebuah email yang dikirim pengirimnya seharusnya tidak dapat dibaca orang lain sebelum sampai ke tujuannya.

c. Authentication

Hal ini menekankan mengenai keaslian suatu data/informasi, termasuk juga pihak yang memberi data atau mengaksesnya tersebut merupakan pihak yang dimaksud. Contohnya seperti penggunaan PIN atau *password*.

d. Availability

Aspek yang berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sebuah sistem inforrmasi yang diserang dapat menghambat ketersediaan informasi yang diberikan.

e. Access Control

Aspek ini berhubungan dengan cara pengaksesan informasi. Hal ini biasanya berhubungan dengan klasifikasi data (*public, private confidential, top secret*) dan *user* (*guest, admin, top manager*, dsb.), mekanisme *authentication* dan juga *privacy*. Seringkali dilakukan dengan menggunakan kombinasi *user ID/password* dengan metode lain seperti kartu atau *biometrics*. Jaringan *wireless* dalam penerapannya tidak memberikan nilai tambah.

1. METODE PENELITIAN

Data Primer

Data primer adalah data *kualitatif* yang diperoleh dari hasil analisa pada infrastruktur jaringan yang menjadi sampel, misalnya berupa hasil *scanning*, jumlah dan tipe *vulnerability*, jenis serangan yang sering muncul dalam jaringan, atau data yang diperoleh melalui wawancara dengan pengelola seperti jumlah aset yang ada, ketersediaan dokumen kebijakan *(policy)*, daftar SDM yang mengelola, dan lain sebagainya. Data primer yang diperoleh sebagai bahan *assessment* adalah jumlah titik akses poin beserta

informasinya serta dokumen kebijakan keamanan yang digunakan di masing-masing fakultas yang menjadi objek penelitian.

Data Sekunder

Pemahaman teoritis yang didapat selama mengikuti studi. studi literature atau referensi lain (milist atau forum keamanan yang disediakan dalam situs-situs internet dan lain-lain) juga merupakan tambahan wawasan dan pengetahuan mengenai keamanan system informasi jaringan *wireless*.

Perangkat Lunak

Perangkat lunak *aircrack-ng 1.1* dan *wireshark* digunakan pada saat melakukan *cupture* data yang berjalan di *system operasi Linux Ubuntu Marvik 10.10.*

Perangkat Keras

Perangkat keras yang digunakan untuk menjalankan *tools* tiatas. Detail dari *hardware* yang digunakan untuk melakukan analisis keamanan jaringan *wireless* adalah sebagai berikut:

1. Komputer atau netbook dengan spesifikasi :
   a. Intel Atom Processor N450 1.66GHz
   b. 1 GB Memory DDR2 RAM
   c. 160 GB hardisk
   d. Broadcom STA wireless driver
2. System operasi yang digunakan adalah *Linux Ubuntu Marvix 10.10.*

2. HASIL DAN ANALISA

Langkah penelitian dapat di jabarkan sebagai berikut:

1. Melakukan *capture* data menggunakan *aircrack-ng* dan *wireshark* untuk mengetahui titik akses poin yang terdapat di tiap fakultas.
2. Melakukan wawancara kepada *admin* untuk mendapatkan beberapa informasi-informasi tambahan terhadap titik akses poin dan kebijakan yang telah diberlakukan.

4.2.1 Aircrack-ng

Untuk menjalankan atau *mengcrack* kunci WEP akses poin, kita membutuhkan sekumpulan bidang *initialization vector* (IV). Jaringa network yang normal tidak secara khusus menghasilkan IV ini dengan cepat. Penulis harus melakukan teknik injeksi untuk menaikan kecepatan proses. Injeksi ini melibatkan *access point* (AP) untuk menyeleksi kelebihan paket yang akan ditangkap dengan kecepatan yang sangat tinggi. Proses ini sangat singkat dalam penangkapan paket data.

Step dasar sebelum memulai :

1. *Start wireless inter face* pada monitor mode on AP channel yang *spesifik.*
2. Tes kemampuan injeksi pada *wireless device ke access point.*
3. Gunakan aireplay-ng untuk melakukan pengalihan *authentication* dengan AP.
4. Start *airodump-ng* pada *chanel AP* dengan *BSSID filter*

untuk mengumpulkan IV baru yang unik.

5. *Start aireplay-ng* pada ARP permintaan ulang mode pada paket injeksi.
6. *Run aircrack-ng* untuk *crack* kunci menggunakan koleksi IV.

software aircrack ini dijalankan di *terminal* atau *konsol* dengan beberapa tahapan sebagai berikut:

1. melakukan seting terhadap *wireless card.*

   Seting *wireless card* dapat dilakukan pada *terminal* dengan mengetikan perintah seperti Gambar 4.1.:

```
$ sudo airmon-ng stop eth0
```

Gambar 4.1. Perintah seting *wireless card*

Sistem akan merespon perintah tersebut seperti pada Gambar 4.2.

```
Interface    Chipset        Driver

wifi0        Atheros        madwifi-ng
ath0         Atheros        madwifi-ng VAP (parent: wifi0)  (VAP destroyed)
```

Gambar 4.2 tampilan awal menjalankan *aircrack-ng.*

Pada *command* tersebut menjelaskan bahwa mematikan *wireless card* apabila berjalan pada mode monitor. Perintah *iwconfig* digunakan untuk memastikan tidak ada "*athx*" yang lain, maka sistem akan merespon seperti Gambar 4.3.

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.
```

Gambar 4.3. tampilan perintah *iwconfig*

Selanjutnya *wireless card* dihidupkan kembali ke mode monitor dengan *command* seperti pada Gambar 4.4.

```
$ sudo airmon-ng start wifi0 9
```

Gambar 4.4. Perintah mengaktifkan wifi

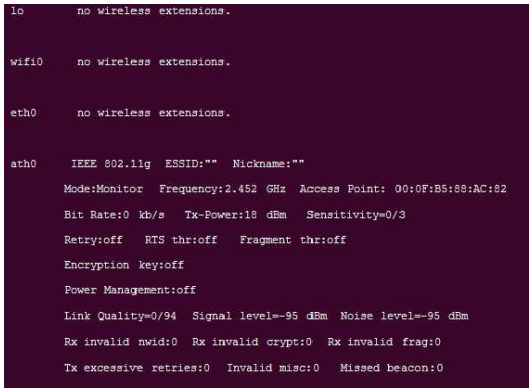
Sistem akan merespon perintah tersebut seperti pada Gambar 4.5.

```
Interface    Chipset        Driver

wifi0        Atheros        madwifi-ng
ath0         Atheros    madwifi-ng VAP  (parent: wifi0) (monitor mode enabled)
```

Gambar 4.5. Pendeteksian jaringan aktif

Masukan perintah *iwconfig* untuk memastikan tidak ada "*athx*" yang lain, maka sistem akan merespon perintah tersebut seperti pada Gambar 4.6.



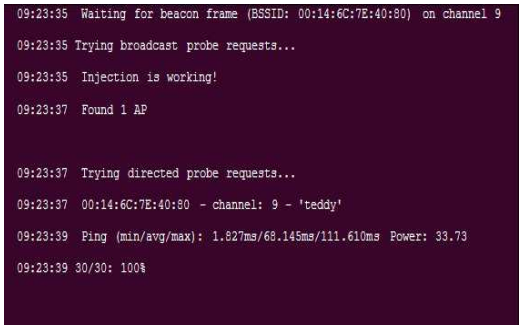
Gambar 4.6. Hasil konfigurasi ath0

2. melakukan *capture* data

   Capture paket digunakan dengan memasukkan *command* seperti Gambar 4.7.:

Gambar 4.7. Perintah injeksi tes

Sistem akan merespon perintah tersebut seperti Gambar 4.8.



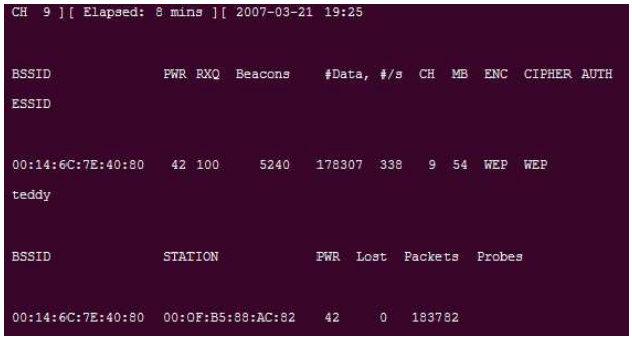
Gambar 4.8. Hasil langkah untuk menjalankan tes injeksi

3. melakukan *configurasi BSSID*

   Cracking WEP dilakukan dengan menjalankan perintah seperti Gambar 4.9.

Gambar 4.9. Perintah konfigurasi BSSID

Sistem akan merespon perintah tersebut seperti Gambar 4.10.

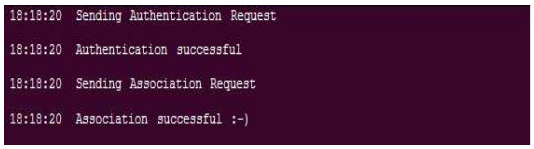


Gambar 4.10. Hasil injeksi tes BSSID

Selanjutnya memberikan perintah penginjeksian dengan data seperti pada Gambar 4.10. Sehingga dilanjutkan dengan perintah seperti ditunjukan pada Gambar 4.11.

Gambar 4.11. Perintah injeksi tes *aireplay-ng*

Sistem akan merespon perintah tersebut seperti pada Gambar 4.12

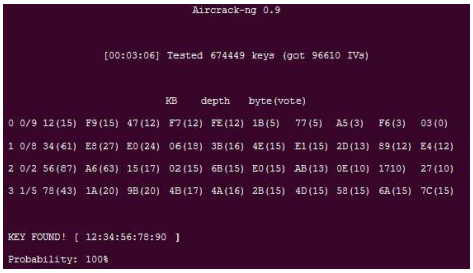


Gambar 4.12. Injeksi tes

4. Melakukan *cracking* data seperti Gambar 4.13.

Gambar 4.13. Perintah *aircrack-ng*

Sistem akan merespon perintah tersebut seperti pada Gambar 4.14.

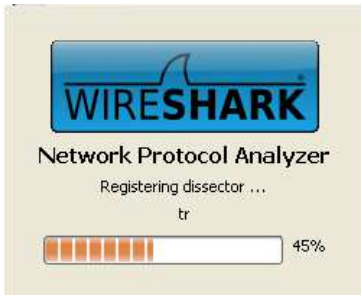


Gambar 4.14. Tampilan hasil *aircrack-ng*

4.2.2 Wireshark

Beberapa tahapan untuk menjalankan *wireshark* dapat di jabarkan sebagai berikut:

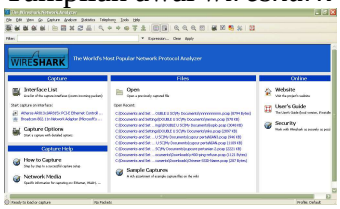
1. Start *wireshark*



Gambar 4.19 *start wireshark*

Gambar 4.19 merupakan awal *start wireshark* yang sedang *meload* komponen-komponen yang diperlukan

2. Tampilan awal *wireshark*



Gambar 4.20 tampilan awal *wireshark*

Gambar 4.20 merupakan tampilan *wireshark* dengan berbagai macam menu sebelum melanjutkan kecapture data.

3. Mulai *capture* data

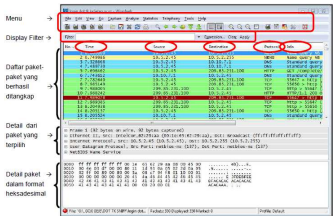
Capture data bisa di mulai dengan mengeklik langkah sebagai berikut:

Gambar 4.21 tampilan *interface*

Berikut adalah gambar dari hasil langkah diatas:

Gambar 4.21 merupakan tampilan *interface* diamana sebelum malakukan *capture* data kita harus memilih diantara *Atheros* atau *Broadcom*.

Pilih *start* untuk menjalankan *capture* data, maka tampilan akan berubah menjadi sebagai berikut:



Gambar 4.22 penjelasan dari tampilan *wireshark*

Gambar 4.22 merupakan penjelasan dari tampilan *wireshark*

4.3 Pembahasan

4.3.1 Analisa *Vulnerability*

Kelemahan yang dianalisa adalah kelemahan yang terdapat pada perangkat software dan pada hasil data *aircrack-ng,* dan *wireshack.*

4.3.1.1 *Vulnerability aircrack-ng*

Dalam melakukan proses ini *aricrack-ng* tidak dapat berjalan dan berikut adalah beberapa penyebab nya:

1. Didalam *ubuntu mervik 10.10* menggunakan *Broadcom STA wireless driver* sedangkan *aircrack-ng* dalam sinyal lemah tidak dapat berjalan menggunakan perangkat *Broadcom* tersebut dan harus menggunakan perangkat *Atheros.*

4.3.1.2 *Vulnerability wireshark*

Proses *wireshark* di lakukan bertujuan untuk mengetahui beberapa informasi yang terdapat pada suatu titik akses poin. Informasi-informasi tersebut dapat digunakan sebagai wadah untuk melakukan serangan-serangan keamanan terhadap titik akses poin.

3. Kesimpulan

1. Pada sinyal yang lemah *aircrack-ng* dapat berjalan dengan menggunakan *atheros card*, sedangkan *Broadcom* hanya bisa berjalan pada sinyal kuat dan stabil.
2. *Software wireshark* dapat berjalan mulus, karena *wireshark* dapat berjalan pada sinyal yang kurang stabil.

DAFTAR PUSTAKA

Adhitya, T.H. 2008. *Tips Untuk Wireless Security* http://www.t1to.com/2008/09/tips-untuk-*wireless*-security.html. Diakses tanggal 19 Oktober 2011.

Barken, L., Ermel, E., Eder, J., Fanady, M., Mee, M., Palumbo, M., Koebrick, A. *Wireless Hacking Projects for Wi-Fi Enthusiasts*. 2004. Syngress Publishing, Inc. Rockland. MA.

Fadils, 2008. *Network Security Wheel*. http://fadils.wordpress.com/2008/06/03/network-security-wheel/. Diakses tanggal 19 Oktober 2011.

Hurley, C., Puchol, M., Rogers, R., Thornton, F. 2004. *WarDriving: Drive, Detect, Defend: Guide to Wireless Security*. Syngress Publishing. Rockland, MA. Insecure.org. 2009. *Free Security Scanner For Network Exploration & Security Audits*. http://nmap.org/. Diakses tanggal 2 Oktober 2009.

Komu, M; & Nordström T. 1999. Known Vulnerabilities in *Wireless* LAN Security. http://www.niksula.hut.fi/~mkomu/docs/*wireless*lansec.html. Diakses tanggal 6 Oktober 2009.

Kurose, F.J; & Ross, W.K. 2000. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison Wesley Publishing Company

Martin, 2009. *Wireless* Network Scanner inSSIDer. http://www.ghacks.net/2009/07/03/*wireless*-network-scanner-inssider/. Diakses tanggal 15 Oktober 2011.

Mateti, P. 2005. *Hacking Techniques in Wireless Networks.*

http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/*Wireless*Hacks/Mateti-*Wireless*Hacks.htm. Diakses tanggal 10 November 2011.